MidSouth eHealth Alliance Policies

R1	Registration: Registration Policy (contains form of Registration Application/Agreement)	
E1	Enrollment: Alliance Confidentiality Statement and Policy	Signed by all authorized users. Asserts sensitive and confidential nature of information, use because of affiliation or participant. Urges appropriate precautions for use. User agrees to confidentiality, use only for direct patient care within role and scope; prohibits disclosure to unauthorized individuals. Acknowledges that terms have been explained and that consequences may include reporting to authorities, change in relationship to the Alliance, termination of access, personal liability, and fines or imprisonment under federal laws. Explains where further information can be obtained for clarification. Emphasizes obligation to report any breaches whether inadvertent or intentional. Emphasizes that reporting will not incur any retaliation.
E2	Enrollment: Secure ID Request Form	Request for SecureID token made to Vanderbilt University as vendor. Participants agree to Vanderbilt University's policies for remote access. This token device strengthens identification management. User ID and Password alone will not suffice. One must have a SecureID for access.
E3	Enrollment: Terms of Use Form	Signed by each user receiving a Secure ID. Re-asserts that patient data will be used only for the purpose of providing patient care; acknowledges the pilot evaluation of a test system in the context of patient care. States that inaccuracies are possible and mentions risks associated with merging of data. Asserts clinician judgment and responsibility. Restricts use to network for specific patient in context of care and requires that information not be displayed in public areas easily seen by unauthorized users. Requires shredding of extraneous hardcopies with patient-specific information.
E4	Enrollment: User Set Up Information Chart	Includes users identifier information, access, role, and supervisor information.
E5	Enrollment: Vanderbilt Confidentiality Agreement	Standard agreement employed in clinical settings at Vanderbilt. Restricts use to job function, prohibits disclosure, and restricts use within all legal and Vanderbilt policies. Requires reporting to supervisor of any potential compromise of confidential information. Sets restrictions on use of user ID and prohibits disclosure to unauthorized individuals. User accepts responsibilities for activities taken using their passwords and access codes. Alerts user of de-activation of their ID if their role changes. Also acknowledges right to audit use. Alerts user to possible disciplinary actions if there are violations.
G1	Governance: Policy on Policies and Procedures	A four-page document defining how policies will be instituted and reviewed. Defines stakeholders, including the MidSouth eHealth Alliance, the Agency for Healthcare Research and Quality, and other groups. Articulates who policies apply to and how exceptions can be made.
G2	Governance: Coordination of the Alliance Policies	States that the Alliance and each Participant shall, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the

	and Participants' Policies	confidentiality and security of individually identifiable health information and establishing certain individual privacy rights. The Alliance and each Participant shall use reasonable efforts to stay abreast of any changes or updates to and interpretations of such laws and regulations to ensure compliance. Declares that each Participant shall, at all times, comply with all applicable Policies and Procedures. These Policies and Procedures may be revised and updated periodically. Participant will receive written notification of revisions and updates consistent with the requirements of the Participation Agreement. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these Policies and Procedures. States that each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and the Alliance Policies and Procedures.
G3	Governance: Privacy and Security Policy	Critical document that sets forth general requirements for privacy and security. Establishes need for each participant to have their own policies and procedures and coordinate with the Alliance. Focuses on notification to patients and means for "opting out" of the data sharing demonstration project. Provides sample patient notification and "opt out" consent language as well as specific policies and procedures that must be adhered to. Covers use and disclosure, information subject to special protection, amendment of data, requests for restrictions. In the area of use and disclosure, describes compliance with law, purposes for which information can be used, compliance with Alliance procedures, audit logs, and authentication mechanisms. A fact sheet is provided as an amendment and will be published separately.
G4	Governance: Conditions to be Met Before a New Data Provider's Data May be Used	Sets for the means by which the Alliance will work with new publishers of data. Addresses Alliance's commitment to work on technical issues, coordinate reliable data feeds, and ensure appropriate mappings of data into the record locator and access services. States that it is the responsibility of the publisher to determine the quality of information submitted. Sets for requirements that must be met before data are made available, including, compliance with all policies and procedures, agreement to privacy and security policies, means for allowing patients to "op out," means for data quality assurance, and submission of an ongoing data quality assurance plan.
G5	Governance: Roles and Responsibilities	A simple document that states that the roles of the participants are specified by the participation agreement and may be supplemented by future policies. States that both the Alliance and participants each must designate an individual or individuals from their respective organizations to address privacy and information security matters and that such designations will be provided to all parties before data are shared.
G6	Governance: User Access	This document states how users will be added to and removed from participation in the data sharing project. The Alliance will maintain a user access table in the Alliance System. Access and termination of access adding and removing users will be managed by a formal process, in which an authorized request to add or remove an Authorized User is sent to the Alliance by an individual designated to play this role. This individual is that of a "data custodian" for

		participant information and is responsible for maintenance of all authorized users from the participating institution. The Alliance and each Participant will validate user lists at pre-defined intervals and will be responsible for reporting according to set policies. The Alliance will support the enrollment of individuals as authorized users through the participant's data custodian. Each custodian will retain original forms and each custodian will be equally responsible for removing participants in a timely manner and maintaining records and communications of removals. The Alliance reserves the right to remove an Authorized User's or Participant's access to the Alliance System and Alliance Services as it deems necessary. Each Participant may request a review of such removal by the Alliance Operations Committee. The Alliance asserts its responsibility for the physical safety and security of its file management system and all its supporting hardware and infrastructure components.
G7	Governance: Auditing and Reporting	This document sets forth how audit logs from the Alliance will be communicated to participants. It describes both the frequency and format of these reports and states how long the Alliance will maintain such logs. The document asserts the right of participants to request additional detail over and above the standard report. The document also states the Alliance's commitment to develop audit alerts and reporting for non-standard activity such as access from an unauthorized IP address.
G8	Governance: Mitigation	This document declares the commitment of each participant to implement a process of mitigation and to take appropriate remedial action, to the extent practicable, any harmful effect that is known to the participant of a use or disclosure of health information involving the Alliance System or Alliance Services in violation of applicable laws and/or regulations and/or the Policies and Procedures by the Participant, or its workforce members, agents, and contractors. It describes some of the steps participants could take as well as requirements for disclosure to the Alliance of inappropriate use of disclosure. It emphasizes the need to comply with all laws requiring notification and mitigation. The document also describes the Alliance's process to mitigate and respond in a similar fashion.